



CHỦ ĐỀ 2:

BẢO VỆ THÔNG TIN VÀ CÁC TÀI KHOẢN TRỰC TUYẾN

Bài 3: Kết nối số an toàn





MỤC TIÊU:

- Hiểu về các kết nối số, bao gồm sử dụng Internet và truy cập website
- Nhận biết được mức độ an toàn của các kết nối số

Với sự phát triển vượt bậc của công nghệ và Internet, việc bảo vệ thông tin cá nhân và dữ liệu trực tuyến ngày càng trở nên quan trọng. Một kết nối số an toàn, bao gồm việc sử dụng Internet và truy cập website đúng cách, không chỉ giúp bạn tránh được các mối đe dọa như vi-rút, phần mềm độc hại và tấn công mạng, mà còn bảo vệ thông tin cá nhân khỏi nguy cơ bị lạm dụng hoặc đánh cắp.

1. Truy cập mạng Internet an toàn

1.1. Chúng ta kết nối với Internet như thế nào?

Trong ngôi làng truyền thống, mạng lưới giao thông và các phương tiện vận chuyển giúp mọi người kết nối, gặp gỡ và chia sẻ thông tin. Tương tự, trong “ngôi làng thế giới số,” kết nối Internet đóng vai trò như các mạng lưới và phương tiện giao thông, giúp chúng ta tiếp cận thông tin, tương tác và mở rộng thế giới của mình.

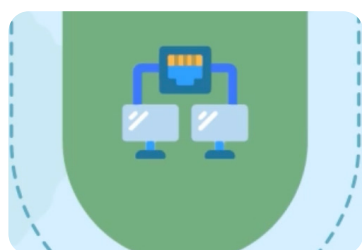
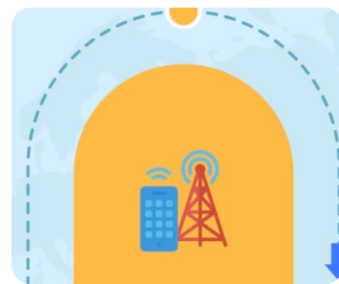


Sau đây là một số kết nối Internet thông dụng nhất:



Kết nối Internet không dây (Wi-Fi): Sử dụng router để phát sóng Wi-Fi, cho phép các thiết bị như điện thoại, laptop, và máy tính bảng kết nối Internet không dây trong phạm vi nhất định. Thông thường Wi-Fi cho phép nhiều người có thể truy cập, giống như các phương tiện công cộng như tàu hỏa, xe buýt, hay ô tô khách...

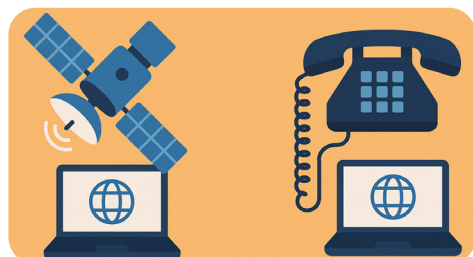
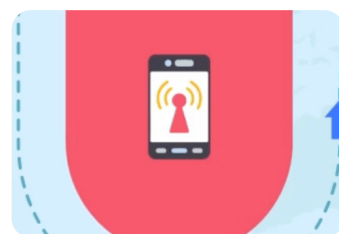
Kết nối Internet có dây (mạng LAN): Sử dụng cáp mạng để kết nối trực tiếp các thiết bị với Internet. Kết nối LAN giống như đi trên một con đường riêng, nơi bạn không cần lo bị kẹt xe hay chia sẻ băng thông với quá nhiều người.



Kết nối qua mạng di động (3G, 4G, 5G):

Đây là các kết nối Internet thông qua đăng ký dịch vụ với các nhà mạng đối với các thuê bao di động cá nhân. Kết nối Internet qua mạng di động giống như di chuyển một cách linh hoạt và bất cứ khi nào bằng các phương tiện cá nhân như xe đạp, xe máy hay ô tô riêng.

Kết nối qua Hotspot di động: Một thiết bị hoặc điện thoại thông minh chia sẻ kết nối mạng di động thành Wi-Fi để các thiết bị khác sử dụng. Tham gia kết nối qua Hotspot di động giống như bạn đi chung hoặc đi nhờ phương tiện của người khác để tham gia giao thông.



Ngoài ra, chúng ta sẽ còn có thể thấy một số kết nối Internet khác như kết nối qua vệ tinh, qua mạng dial up (kết nối qua đường dây điện thoại cố định)...

SUY NGẪM

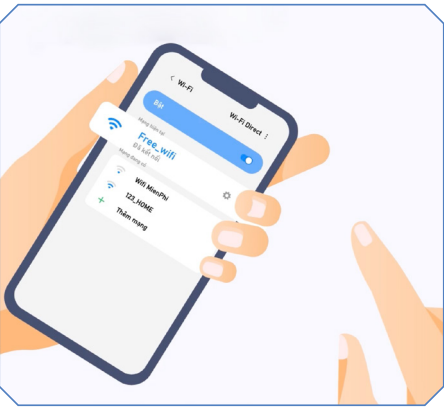
Bạn có những thiết bị nào có thể truy cập Internet? Bạn thường sử dụng những loại kết nối Internet nào?

1.2. Kết nối Internet Wi-Fi an toàn

Trong số các loại kết nối Internet đã đề cập ở trên, Wi-Fi là kết nối mà chúng ta sử dụng phổ biến và thường xuyên nhất. Tuy nhiên, đây cũng là loại kết nối tiềm ẩn nhiều rủi ro và nguy cơ nhất.

Wi-Fi là một công nghệ mạng không dây cho phép các thiết bị như điện thoại, máy tính, máy tính bảng và nhiều thiết bị khác kết nối Internet mà không cần cáp. Với tốc độ cao, phạm vi kết nối rộng, và khả năng hỗ trợ nhiều thiết bị cùng lúc, Wi-Fi đã trở thành một trong những phương thức phổ biến để truy cập Internet tại nhà, văn phòng, trường học, quán cà phê và nhiều không gian công cộng. Tuy nhiên, không phải kết nối Wi-Fi nào cũng an toàn như nhau.

Chúng ta có thể phân biệt *hai loại kết nối Wi-Fi* sau:



Kết nối công khai: là các mạng không yêu cầu mật khẩu để đăng nhập. Đây giống như xe buýt miễn phí hoặc tàu công cộng không cần vé, nơi ai cũng có thể lên sử dụng. Mặc dù tiện lợi, nhưng bạn phải đối mặt với nhiều rủi ro, vì bất kỳ ai cũng có thể “lên tàu”

và có ý đồ xấu. Những người khác đang sử dụng trên cùng một mạng có thể đánh cắp thông tin bạn gửi qua mạng hoặc theo dõi những gì bạn đang làm.

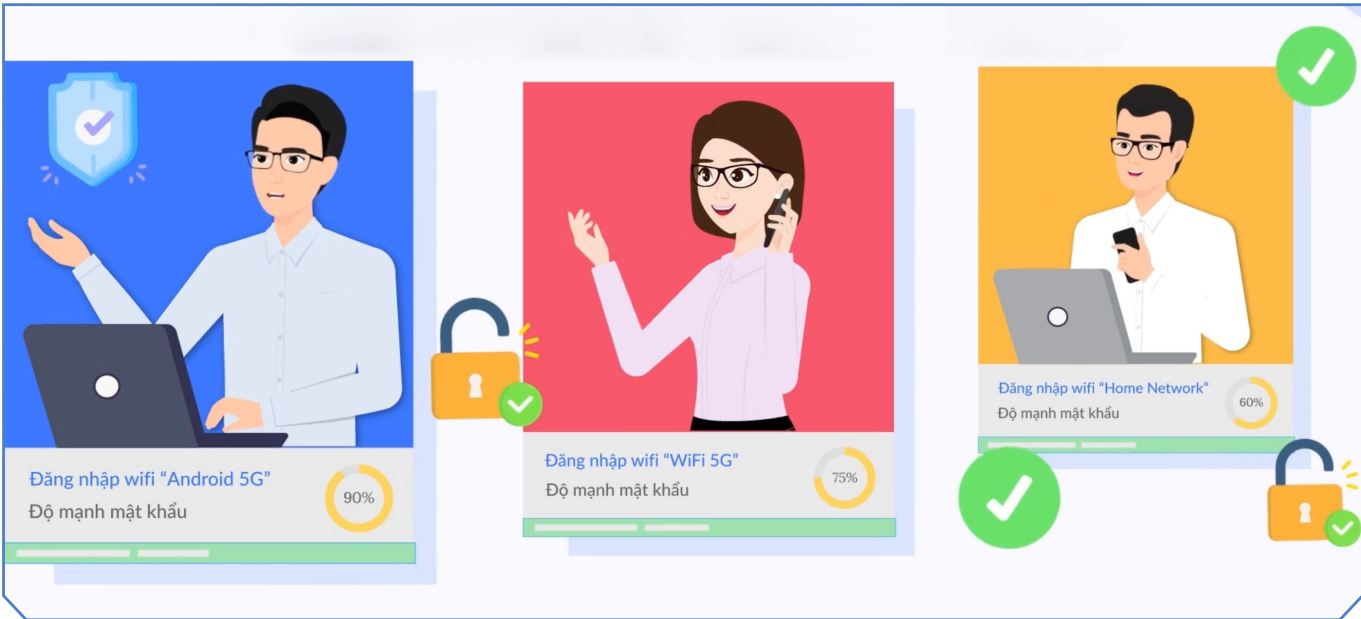
Hãy xem xét ví dụ sau: Chị Lan đang ở quán cà phê và thấy tên mạng Internet của quán hiển thị khi tìm kiếm kết nối Wi-Fi. Chị Lan có thể kết nối với mạng này luôn và không cần nhập bất cứ thông tin mật khẩu nào. Kết nối mạng đó là một kết nối công khai. Khi kết nối với mạng này thì chị Lan có thể đối mặt với rủi ro là kẻ xấu sử dụng các kỹ thuật để xem trộm



và biết toàn bộ thông tin chị Lan gửi qua mạng và theo dõi những gì chị Lan đang làm.



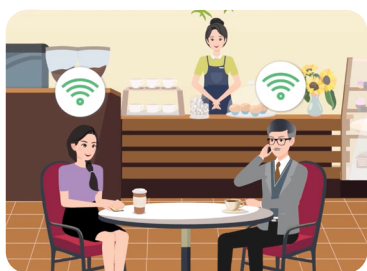
Kết nối riêng tư: là các mạng yêu cầu mật khẩu để tham gia, đã bật mã hóa đầu cuối. Đây giống như xe buýt hoặc tàu yêu cầu mua vé, nơi chỉ những người có vé (mật khẩu) mới được phép sử dụng. Vé này đảm bảo rằng không phải ai cũng có thể “lên tàu”, giảm nguy cơ gặp người xấu trên chuyến đi. Đây là kết nối an toàn, đáng tin cậy hơn vì cung cấp khả năng bảo vệ tốt hơn. Điều này có nghĩa là bạn sẽ biết rõ hơn những ai đang sử dụng mạng, so với nếu đó là mạng mở miễn phí hoàn toàn. Mạng sử dụng mật khẩu càng mạnh thì càng an toàn.



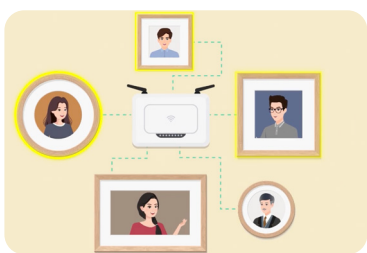
Lưu ý rằng, cho dù kết nối Wi-Fi công khai hay riêng tư, bạn chỉ nên kết nối với mạng Wi-Fi được cung cấp bởi những người hoặc tổ chức bạn tin tưởng. Tất cả lưu lượng truy cập trên mạng Wi-Fi đều đi qua bộ định tuyến (thiết bị trung gian giúp kết nối các thiết bị khác với Internet), nên chủ sở hữu mạng có thể giám sát hoặc ghi lại lưu lượng truy cập web của bạn. Trong trường hợp kẻ xấu tạo ra một Wi-Fi giả mạo để bạn truy cập thì thông tin của bạn sẽ có nguy cơ bị xâm phạm. Ví dụ: Nếu bạn đang ở quán

cà phê và thấy mạng của một trường học nào đó ở cách đó khoảng 2 km thì đó cũng có thể là một mạng giả mạo. Hoặc khi chị Lan ngồi ở quán cà phê ABC, mạng chính thức của quán là *ABC_Wi-Fi* nhưng mạng giả mạo có thể sẽ gần giống tên mạng chính thức như *ABC_Free*. Trong trường hợp này, chị Lan nên xác nhận lại về tên Wi-Fi chính thức với nhân viên của quán.

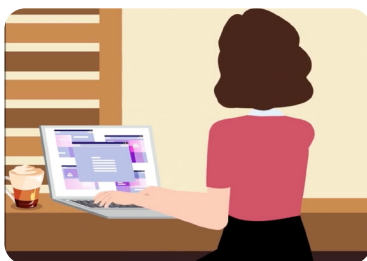
Nhìn chung, để kết nối với một mạng Wi-Fi an toàn, hãy xem xét những yếu tố sau:



Ai là **chủ sở hữu** mạng Wi-Fi tại nhà của bạn? Tại trường học? Tại quán cà phê? Bạn có biết những người hay tổ chức này không? Bạn có tin tưởng họ không?



Có những ai **có thể truy cập** mạng này? Ít người hay nhiều người (công khai hay riêng tư)? Liệu họ có đáng tin cậy không?



Bạn dùng mạng đó để **làm gì** (có gửi đi các thông tin quan trọng không)? Liệu có rủi ro gì không?

Khi quyết định tham gia một mạng nào đó mà bạn chưa chắc chắn về mức độ an toàn của nó thì bạn cần phải *xem xét về những rủi ro mà bạn có thể gặp phải*. Bạn có thể cân nhắc giữa nguy cơ tài khoản hay thông tin bị xâm phạm và sự thuận tiện khi tham gia một mạng có sẵn và không yêu cầu mật khẩu. Đồng thời, hãy luôn cân nhắc mình sẽ làm gì khi sử dụng kết nối mạng đó.

Tuy nhiên, trên thực tế, không phải lúc nào chúng ta cũng ở nhà để dùng Wi-Fi tại nhà cho những hoạt động trên mạng cần độ bảo mật cao như chuyển khoản hay đăng nhập

vào những tài khoản quan trọng. Trong trường hợp này, bạn có thể cân nhắc một số giải pháp sau:



Dùng dữ liệu di động (3G/4G/5G) thay vì Wi-Fi công cộng.



Sử dụng **VPN**¹ để mã hóa đường truyền dữ liệu. VPN sẽ giúp bảo vệ dữ liệu cá nhân bằng cách mã hóa toàn bộ dữ liệu truyền và nhận trên Internet, ngăn chặn kẻ xấu theo dõi hoạt động trực tuyến của bạn. Đồng thời, VPN cũng che giấu địa chỉ IP thật, giúp bạn duyệt web an toàn và ẩn danh hơn. Để sử dụng VPN, hãy chọn một dịch vụ uy tín, tải ứng dụng về thiết bị, cài đặt và đăng ký tài khoản. Hiện có cả dịch vụ VPN miễn phí và trả phí.

SUY NGẪM

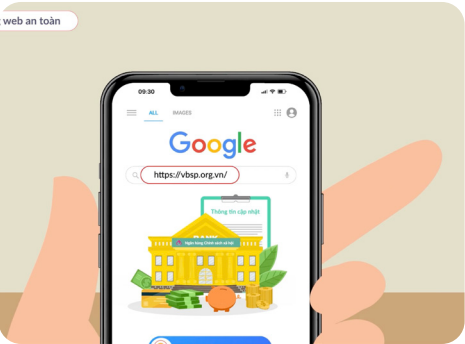
Chị Lan cần chuyển khoản cho người thân qua ngân hàng điện tử. Theo bạn, chị Lan nên dùng mạng nào để an toàn nhất? Wi-Fi tại quán cà phê hay Wi-Fi tại nhà?

(Gợi ý: Wi-Fi tại nhà là an toàn nhất và không nên gửi qua mạng Wi-Fi của quán cà phê vì đây là thông tin nhạy cảm mà kẻ xấu có thể lợi dụng để lừa đảo hoặc đánh cắp thông tin của bạn. Trong trường hợp đang ở bên ngoài và chỉ có Wi-Fi tại quán cà phê, chị Lan nên cân nhắc dùng kết nối 3G/4G/5G cá nhân để thực hiện giao dịch chuyển khoản).

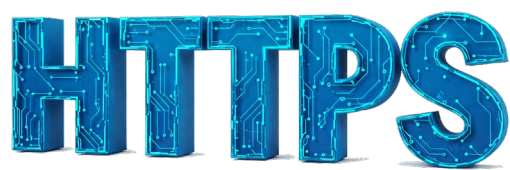
1 VPN (Virtual Private Network) là một công nghệ tạo ra một kết nối mạng riêng tư giữa thiết bị của bạn và Internet. Khi sử dụng VPN, dữ liệu của bạn được mã hóa và truyền tải qua một “đường hầm” bảo mật, giúp bảo vệ bạn khỏi sự theo dõi và xâm nhập từ các bên thứ ba

2. Truy cập trang web an toàn

Hãy cùng theo dõi tình huống sau: Anh Khoa, 40 tuổi, đang muốn tìm hiểu thêm các thông tin cập nhật của Ngân hàng Chính sách xã hội như lãi suất cho vay hay quy trình cho vay các chương trình. Anh Khoa truy cập trang web của Ngân hàng Chính sách xã hội, với địa chỉ truy cập: <https://vbsp.org.vn/>. Đây là một trang thông tin điện tử, hay nói cách khác là một trang web cung cấp tin tức trực tuyến, giúp anh Khoa dễ dàng tiếp cận thông tin mọi lúc, mọi nơi.



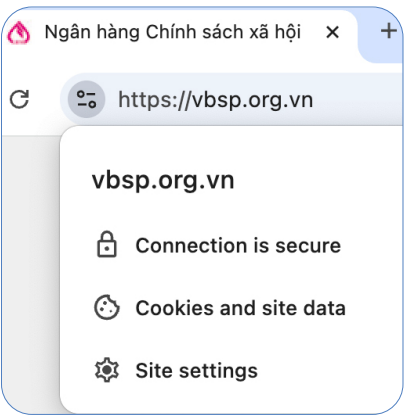
Trang web (Website) là tập hợp các trang thông tin được liên kết với nhau, có thể truy cập qua Internet thông qua một trình duyệt web. Trang web có thể phục vụ nhiều mục đích khác nhau, từ cung cấp thông tin (như báo điện tử), giải trí (xem phim, nghe nhạc), học tập (các nền tảng giáo dục), đến kinh doanh (mua sắm trực tuyến) và giao tiếp (mạng xã hội). Chúng đã trở thành một phần thiết yếu của cuộc sống hiện đại nhờ khả năng lưu trữ và cung cấp thông tin nhanh chóng. Giống như địa chỉ nhà, mỗi trang web có một địa chỉ duy nhất, gọi là *đường dẫn* hoặc *đường link (URL)*.



Các trang web có mức độ an toàn không giống nhau. Một trong những cách để bạn nhận biết mức độ an toàn này là xem xét về **giao thức truyền dữ liệu** hay cách thức truyền dữ liệu giữa bạn và trang web mà trang web đó đang áp dụng. **HTTP** và **HTTPS** là hai giao thức chính cho các trang web, trong đó HTTPS hiện nay là tiêu chuẩn an toàn được sử dụng rộng rãi. Trong trường hợp cần nhập thông tin cá nhân hoặc nhạy cảm (chẳng hạn như mật khẩu, thông tin thẻ tín dụng), bạn chỉ nên thực hiện trên trang web sử dụng giao thức HTTPS. Tại sao lại như vậy?

HTTPS sử dụng chứng chỉ số (SSL/TLS) để xác minh tính hợp lệ của trang web và bảo vệ dữ liệu. Chứng chỉ số này cho phép các trang web **mã hóa dữ liệu** truyền qua mạng Internet. *Mã hóa là gì?* Hãy liên tưởng đến câu chuyện sau: Một vị tướng quân muốn gửi một lá thư bí mật cho đồng minh của mình. Để bảo đảm kẻ thù không thể đọc được nội dung nếu bắt được thư, vị tướng này đã biến các ký tự trong bức thư thành các ký tự khác theo một quy luật mà chỉ ông và đồng minh của mình biết được. HTTPS hoạt động tương tự như vậy. Khi bạn nhập thông tin của mình trên một trang web sử dụng giao thức này, *quá trình mã hóa có thể khiến bên thứ ba khó lòng mà xem được dữ liệu của chúng ta trong quá trình truyền* - nhận vì nó được hiển thị theo một dạng khác.

Làm thế nào nhận biết một trang web sử dụng giao thức HTTPS?



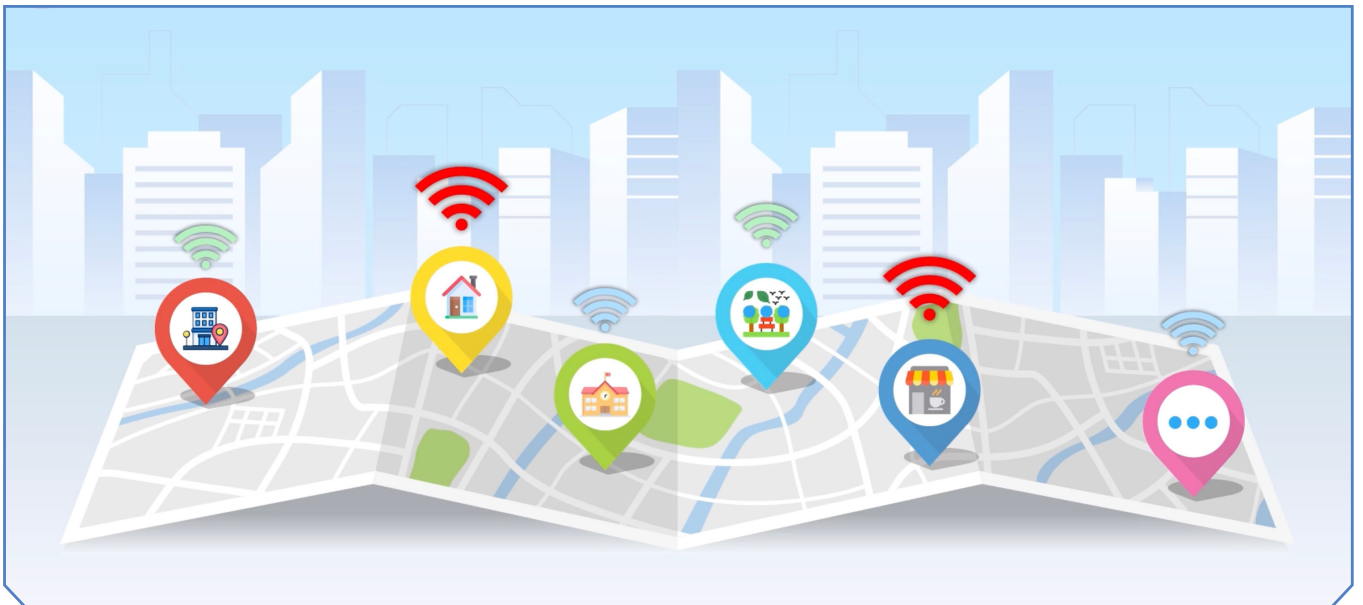
- Các trình duyệt phổ biến như Chrome, Firefox thường hiển thị biểu tượng **ổ khóa** nhỏ  bên cạnh thanh địa chỉ để cho biết trang web đang sử dụng HTTPS.
- Đường dẫn của các trang web này sẽ bắt đầu bằng “https://”.

Lưu ý, *HTTPS không đảm bảo được an toàn tuyệt đối cho chúng ta* vì một số trang web độc hại cũng có thể hỗ trợ HTTPS. HTTPS bảo mật kết nối nhưng không đảm bảo trang web đó là một trang web lừa đảo hay không. Hãy đảm bảo rằng trang web mà bạn truy cập vừa sử dụng giao thức an toàn, vừa đảm bảo chính chủ và uy tín.

SUY NGÃM

Anh Khoa cần đăng ký một khóa học trực tuyến, trang web yêu cầu anh Khoa nhập thông tin cá nhân để đăng ký như họ tên, ngày sinh, số điện thoại, số tài khoản ngân hàng. Anh Khoa có nên nhập không nếu địa chỉ trang web bắt đầu bằng: “https://...”?

(Gợi ý: https:// là giao thức an toàn, tuy nhiên anh Khoa chỉ nên nhập thông tin nếu như anh chắc chắn rằng trang web này là trang web chính thức của đơn vị cung cấp khóa học, đồng thời chủ sở hữu trang web là tổ chức uy tín và đáng tin cậy.)



Nội dung chính cần ghi nhớ

1. Có nhiều loại kết nối Internet bao gồm: Kết nối Internet không dây (Wi-Fi); Kết nối Internet có dây; Kết nối qua mạng di động (3G, 4G, 5G); Kết nối qua Hotspot di động và một số loại kết nối khác.
2. Không phải kết nối Internet Wi-Fi nào cũng an toàn như nhau. Cần phân biệt 2 loại mạng sau:
 - Kết nối công khai là các mạng không yêu cầu mật khẩu để đăng nhập. Đây là kết nối không an toàn, không đáng tin cậy vì những người khác đang sử dụng trên cùng một mạng có thể xem thông tin của bạn. Họ có thể đánh cắp thông tin bạn gửi qua mạng hoặc theo dõi những gì bạn đang làm.
 - Kết nối riêng tư: Yêu cầu mật khẩu để tham gia, đã bật mã hóa. Đây là kết nối an toàn, đáng tin cậy vì cung cấp khả năng bảo vệ tốt hơn.
3. Khi truy cập bất kỳ mạng Wi-Fi nào, hãy xem xét những yếu tố sau: vị trí hoặc chủ sở hữu mạng, quyền truy cập (hoặc người nào khác được kết nối với mạng đó) và hoạt động (hoặc chúng ta đang làm gì trên mạng đó). Và bạn chỉ nên kết nối với mạng Wi-Fi được cung cấp bởi cá nhân hoặc tổ chức uy tín và đáng tin cậy.
4. Trong trường hợp cần phải thực hiện các hoạt động trên mạng cần độ bảo mật cao, hãy cân nhắc các giải pháp sau:
 - Dùng dữ liệu di động (4G/5G) thay vì WiFi công cộng.
 - Sử dụng VPN để mã hóa đường truyền dữ liệu
5. Bạn chỉ nên nhập thông tin nhạy cảm (chẳng hạn như mật khẩu, thông tin thẻ tín dụng) trên trang web có tiền tố “https://” tuy nhiên HTTPS không đảm bảo được an toàn tuyệt đối cho chúng ta vì một số trang web độc hại cũng có thể hỗ trợ HTTPS.